



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,599	03/09/2004	Weishi Feng	MP0386	1797
26703	7590	01/27/2009	EXAMINER	
HARNESS, DICKEY & PIERCE P.L.C.			SAN JUAN, MARTINJERIKO P	
5445 CORPORATE DRIVE				
SUITE 200			ART UNIT	PAPER NUMBER
TROY, MI 48098			2432	
			MAIL DATE	DELIVERY MODE
			01/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/796,599	FENG, WEISHI	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 20 October 2008.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-86 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-86 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 09 March 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____. | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

This is a response to Applicant's Remarks filed on October 20, 2008.

Claims 1-86 are currently pending.

Response to Arguments

1. Applicant's arguments filed October 20, 2008 have been fully considered but they are not persuasive.

Regarding claim 1, Sims III teaches a public key decryption module that controls decryption of an encrypted content key for a secure hard drive using a private key to generate a content key [Sims 12: 1-4 –preselection of a device secret key to decrypt the encrypted content key teaches the limitation to the extent how the limitation is supported by the Applicant's Specification in Par 0029.] [Sims 12: 19-21 --The device secret key is used to generate a content key by decrypting an encrypted content key.]. Sims III has the capability of preventing access of encrypted data by other HDDs when placed in a computer because each HDD has its own device secret key for use in controlling the decryption. Searle teaches the private key generated based on a device specific identification (ID) [Searle 5: 34-64]. The device specific ID disclosed by Searle is not limited to an identifier that is unique to a computer but rather, it can be any other such device so as long as it is unique and particular from each other [Searle 6: 64], and as disclosed can be a processor ID of the device [Searle 7: 3]. Searle is directed to the encryption/decryption of data performed generally by devices [Searle 8: 5-18] which can be devices other than computers [Searle 8: 5-41]. In the obviousness rejection presented by the Examiner, the secure hard drive disclosed by Sims III is the primary

reference and is the one that is being modified to have its private key generated based on a device specific ID as taught by Searle. Searle is being used merely as a teaching reference that only teaches how a private key is generated based on a device specific ID. From the above reasons, the combination of Sims III in view of Searle would not suggest the encryption of data and generation of corresponding keys by a computer using a computer specific identifier prior to further encryption and use of additional keys by a storage device as alleged by the Applicant, but rather, it would have taught the Applicant's limitations as claimed.

Regarding claim 83, Searle's disclosure of a device specific ID includes that of a processor ID of the device [Searle 7: 3]. Sims III in view of Searle would have taught that the device specific ID would have been the processor ID of a processor belonging to Sims III's hard drive. Furthermore, there is no language in the limitations that the chip ID corresponds to an internal circuit component of a HDD that is typically not visually accessible or easily determinable.

Claim Rejections - 35 USC § 112

1. Claim 80 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claim 80 specifically the limitation that the decryption module generates said content key based on said public key, there is no support in the Applicant's Specification that the public key is used to generate the content key.

2. Claims 1, 20, 31, and 50 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 1, 20, 31, and 50, "the public key decryption module that controls decryption of said encrypted content key for said secure hard drive using a private key to generate a content key" is new. There is no support in the Applicant's Specification of this matter. For purposes of examination, the limitation is interpreted that the public key decryption module generates a content key by decrypting of said encrypted content key using a private key as seen on Par 0029 of the Applicant's Specification.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 1-10, 13-21, 23-27, 29-40, 42-51, 53-67, 69-79, and 81-86 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Searle [US 6683954 B1].

Based on independent claim 1, Sims III teaches an apparatus with a secure hard drive comprising a storage medium [6550011 B1, Col 13, Ln 4] that stores encrypted digital

content and corresponding encrypted content keys [6550011 B1, Col 13, Ln 35]; a public key decryption module that receives one of said encrypted content keys from said storage medium and that controls decryption of said encrypted content key for said secure hard drive using a private key [6550011 B1, Col 12, Ln 1-4 – preselected device secret key] to generate a content key [Sims 12: 1-4 –preselection of a device secret key to decrypt the encrypted content key teaches the limitation to the extent how the limitation is supported by the Applicant's Specification in Par 0029.] [Sims 12: 19-21 -- The device secret key is used to generate a content key by decrypting an encrypted content key.]; and a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key [6550011 B1, Col 11, Ln 50][6550011 B1, Col 18, Ln 5].

However, Sims III does not teach wherein said private key is generated based on a device specific identification (ID).

Searle teaches a private key generated based on a device specific identification (ID) [Searle 5: 34-64].

It would have been obvious to one of ordinary skill in the art at the time of invention to generate the private key of Sims III using a device specific identification (ID) as taught by Searle. The suggestion/motivation for combining would have been to generate keys for fraud prevention [Searle 2: 13-33]. Sims III and Searle are analogous art because it

solves the problem of generating a more secure private key that addresses fraud prevention.

With regard to dependent claim 2, the combined invention of Sims III and Searle teaches the secure hard drive of claim 1, where in said storage medium is a magnetic storage medium [6550011 B1, Col 13, Ln 5][Magnetic, per se, is inherent within the scope of writeable media].

With regard to dependent claim 3, the combined invention of Sims III and Searle teaches the secure hard drive of claim 1, wherein said public key decryption module and said block decryption module are implemented by a system on chip (SOC) [6550011 B1, Col 14, Ln 12].

With regard to dependent claim 4, Sims III teaches the secure hard drive of claim 1 further comprising a content player that receives said decrypted digital content from said block decryption module and that generates at least one of an analog output signal and a digital output signal [6550011 B1, Col 6, Ln 52], and a public key decryption module [6550011 B1, Col 11, Ln 50 -- encryption/decryption engine] that uses a private key [6550011 B1, Col 12, Ln 1 -- device preselected secret key] to generate said content key based on said private key [6550011 B1, Col 12, Ln 20].

Sims III does not teach the secure hard drive further comprising: an identification ID module that provides said specific device ID, wherein said public key decryption module generates said private key using said device specific ID.

Art Unit: 2432

Searle teaches an ID module that provides said specific device ID, wherein said public key decryption module generates a private key using a device specific identification (ID) [Searle 5: 34-64].

It would have been obvious to one of ordinary skill in the art at the time of invention to generate the private key of Sims III using a device specific identification (ID) as taught by Searle. The suggestion/motivation for combining would have been to generate keys for fraud prevention [Searle 2: 13-33]. Sims III and Searle are analogous art because it solves the problem of generating a more secure private key.

With regard to dependent claim 5, the combined invention of Sims III and Searle teaches the secure hard drive of claim 1 further comprising a controller that performs buffer management and timing of read/write operations [6550011 B1, Col 13, Ln 5][Controllers performing buffer management and timing of read/write operations are inherent in writeable storage devices.]

With regard to dependent claim 6, the combined invention of Sims III and Searle teaches a system comprising the secure hard drive of claim 5 and further comprising an external host [6550011 B1, Col 20, Ln 8]; and a control interface that provides a communications interface between said controller and said external host [6550011 B1, Col 20, Ln 48][A control interface is inherent to enable transfer of content as cited.]

With regard to dependent claim 7, the combined invention of Sims III and Searle teaches the system of claim 6, wherein said external host is one of a computer and a portable media player [6550011 B1, Col 19, Ln 30][6550011 B1, Col 20, Ln 8].

With regard to dependent claim 8, the combined invention of Sims III and Searle teaches the hard drive of claim 4 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark [6550011 B1, Col 15, Ln 15].

With regard to dependent claim 9, the combined invention of Sims III and Searle teaches the secure hard drive of claim 1, wherein said storage medium stores a content directory having content directory entries for said content [6550011 B1, Col 19, Ln 6-11], [6550011 B1, Col 13, Ln 22].

With regard to dependent claim 10, the combined invention of Sims III and Searle teaches the secure hard drive of claim 9, wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play [6550011 B1, Col 15, Ln 48-60].

With regard to dependent claim 13, the combined invention of Sims III and Searle teaches the secure hard drive of claim 9 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status [playback is < XXX] enables playback and said inactive status [playback is XXX] disables playback [6550011 B1, Col 15, Ln 5-21].

With regard to dependent claim 14, the combined invention of Sims III and Searle teaches the secure hard drive of claim 9 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content [6550011 B1, Col 13, Ln 25].

With regard to dependent claim 15, the combined invention of Sims III and Searle teaches the secure hard drive of claim 9 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storage medium [6550011 B1, Col 15, Ln 61-65 --Content decryption key, when stored in a separate location from other associated information, is commonly indexed.]

With regard to dependent claim 16, the combined invention of Sims III and Searle teaches the secure hard drive of claim 9 where in at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in a encrypted content block stored on said storage medium [6550011 B1, Col 15, Ln 61-65 --Encrypted content, when stored in a separate location from other associated information, is commonly indexed.].

With regard to dependent claim 17, the combined invention of Sims III and Searle teaches the secure hard drive of claim 1 wherein said content includes at least one of audio, video, and still pictures [6550011 B1, Col 7, Ln 62].

With regard to dependent claim 18, the combined invention of Sims III and Searle teaches the system of claim 6 further comprising a distributed communications network [Col 9, Ln 13]; and a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications network [Col 20, Ln 2][A content distributor is associated with content provider in a "pay per view" system.]

With regard to dependent claim 19, the combined invention of Sims III and Searle teaches the secure hard drive of claim 1, wherein said storage medium contains encrypted content that is pre-stored thereon [6550011 B1, Col 20, Ln 55].

Independent claim 20 is rejected using the same references as claims 1, 2, and 3.

Dependent claim 21 is rejected using the same reference as claim 4 with the limitation regarding a content player that receives said decrypted digital content.

Dependent claim 23, 24, 25, 26, and 27 are rejected using the same reference as claim 5, 6, 8, 9, and 10 respectively.

Dependent claim 29, and 30 are rejected using the same reference as claim 17, and 18 respectively.

Claims 31-40, and 42-49 are rejected using the same references as claims 1-10, and 12-19.

Claims 1-10, and 12-19 is the apparatus with all limitations having the necessary structure and components as disclosed in the specification for performing the function recited in all the limitations of claims 31-40, and 42-49.

Claims 50, 51, and 53-60 are rejected using the same references as claims 20, 21, 23-30.

Claims 20, 21, 23-30 is the apparatus with all limitations having the necessary structure and components as disclosed in the specification for performing the function recited in all the limitations of claims 50, 51, and 53-60.

Claims 61-67, and 69-77 are rejected using the same references as claims 1-6, 8-10, 12-17, and 19.

Claims 1-6, 8-10, 12-17, and 19 is the apparatus with all limitations performing the method of claims 61-67, and 69-77.

Claim 78-79, and 81-83 are rejected because it contains the same subject matter as claim 4. [Chip ID is intrinsic to the device where the chip is being utilized.]

Regarding claim 84, Sims III in view of Searle teaches the secure hard drive of claim 1, wherein said private key is generated during decryption of said encrypted content key [Searle 6: 1-4].

Regarding claim 85, Sims III in view of Searle teaches the secure hard drive of claim 1, wherein said device specific ID is a chip ID of a system on chip of the secure hard drive [Searle 7: 3 --A system on chip is broadly interpreted as a device microprocessor.].

Regarding claim 86, Sims III in view of Searle teaches the secure hard drive of claim 1, wherein said public key decryption module converts said chip ID into said private key using a transformation/manipulation algorithm [Searle 5: 51].

Sims III in view of Searle does not teach a transformation/manipulation algorithm to be a keyed hash function.

Official notice is taken that it is common and well known in the art for a transformation/manipulation algorithm to be a keyed-hash function.

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III in view of Searle by using a keyed hash function as the transformation/manipulation algorithm as it is common and well known in the art. The suggestion/motivation for combining would have been to secure the algorithm of transforming/manipulating the chip ID into the correct private key.

Art Unit: 2432

2. Claims 22, 52, and 80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Searle [US 6683954 B1] and Heer et al [US PN 5999629].

Regarding claim 80, the combined invention of Sims III, and Searle teach the secure hard drive of claim 78, wherein said public key decryption module generates said content key based on a public key [US 6550011 B1, Col 12, Ln 17 – Content key is encrypted using device's public key, which is decrypted using device's secret key].

However the combined invention of Sims III and Searle do not teach wherein said public key decryption module generates a public key based on said private key.

Heer teaches a security module that generates a corresponding public key based from a device's private key [5999629, Col 4, Ln 34-51]

It would have been obvious to one of ordinary skill in the art at the time of invention to further modify the encryption/decryption engine of the combined invention of Sims III and Searle so that a corresponding public key can be generated from said private key.

The suggestion/motivation for combining would have been to cover the device's secret key [5999629, Col 1, Ln 30-40] through the utilization of asymmetric cryptographic keys.

Heer is analogous art because it solves the problem of not revealing the device's secret key in the communication channels.

Dependent claims 22 and 52 are rejected using the same reference as claim 80 because it contains the same subject matter since the public key is generated from the private key, the private key generated using the Chip ID.

3. Claims 11, 41, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Searle [US 6683954 B1] and Nishimoto et al. [US 7380135 B2], hereinafter Nishimoto.

With regard to dependent claim 11, the combined invention of Sims III and Searle teaches the secure hard drive of claim 9.

Sims in view of Searle does not teach wherein at least one of said content directory entries contains a clear content counter that specifies a portion of said corresponding content that is not encrypted [6550011 B1, Col 15, Ln 7].

Nishimoto teaches a directory entry that contains a clear content counter that specifies a portion of said corresponding content that is not encrypted [Nishimoto 3: 46-64].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III in view of Searle to include a content directory entry that contains a clear content counter as taught by Nishimoto. The suggestion/motivation would have been to achieve previewing portions of an encrypted content [Nishimoto 2: 42-49]. Nishimoto is analogous art because it solves the problem for providing for previewing portions of an encrypted content.

Claims 41 and 68 are rejected because it is similar matter to claim 11.

4. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Searle [US 6683954 B1] and Marsh [US 2003/0195891 A1].

With regard to dependent claim 12, Sims III in view of Searle does not teach the secure hard drive of claim 9, wherein at least one of said content directory entries includes a

Art Unit: 2432

content distributor ID field that identifies a content distributor supplying said corresponding content.

Marsh teaches a content directory entry that includes a content distributor ID field that identifies a content distributor supplying said corresponding content [Fig 3, Itm 304]. It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III, in view of Searle, to include an content distributor ID as taught by Marsh. The suggestion/motivation would have been to provide more criteria in classifying and organizing media content in a directory.

5. Claims 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Searle [US 6683954 B1], Nishimoto [US 7380135 B2] and Marsh [US 2003/0195891 A1].

Dependent claim 28 is rejected because it is similar matter as claims 11, 12, 13, 14, 15, and 16 combined.

Conclusion

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan

Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432